REMARKS

Applicants appreciate the thorough examination of the present application as reflected in the Final Official Action mailed January 14, 2005. Applicants appreciate the indication of allowance of Claim 1-28. Applicants, however, submit that Claims 29-66 are also allowable over the cited references.

The IDS

Applicants wish to bring to the attention of the Examiner Information Disclosure Statements that were filed July 13, 2004 and September 28, 2004 in the present case. These Information Disclosure Statements appear in the PAIR system. Applicants request that the Examiner return copies of the PTO-1449 forms that are initialed indicating consideration of these materials with any subsequent communication.

The Claims Are Not Anticipated

Claims 29, 31-44, 48-53 and 55-66 stand rejected under 35 U.S.C. § 102 as anticipated by United-States Patent No. 5,499,298 to Narasimhalu et al. (hereinafter "Narasimhalu"). Final Action, p. 3. Of the Claims, Claims 29, 41, 53, 65 and 66 are independent claims. Applicants will first address each of the independent claims and then address the dependent claims. Applicants will address the independent claims in the order they were addressed in the Official Action.

Claims 29 53 and 66

In response to Applicants' previous argument that Claim 29 utilizes three keys, the Official Action asserts that Claim 29 "is directed to a program that encrypts per request there is no distinction for the use of three keys."

Claim 29 recites:

> 29.   (Currently Amended) A method for controlling access to digital data of a file in a file system having a personal key server, the personal key server carrying out the steps of:
> receiving a request from a requestor to create a file header associated with the file, the request containing **an encryption key utilized to encrypt the digital data**, the encryption key being encrypted with **a personal key**;
> encrypting the encrypted encryption key with a **control key** to provide the file header containing an encryption key encrypted with both a personal key and a control key; and

returning the file header to the requestor.

Claim 29, emphasis added. Applicants have highlighted the portions of Claim 29 that recite the three keys used. The first key is an encryption key utilized to encrypt the digital data. The second key is the personal key utilized to encrypt the encryption key. The third key is the control key that is used to encrypt the encrypted encryption key. Thus, Claim 29 also provides for three encryption keys. As discussed in Applicants' previous response, and as indicated in the Reasons for Allowance on page 10 of the Final Action, the cited reference only describes a system that uses two keys. In contrast, Claim 29 clearly recites the use of three keys. Accordingly, Applicants submit that Claim 29 is patentable over Narasimhalu at least for reasons acknowledged by the Examiner as providing patentability of Claim 17.

Claim 53 is a system claim corresponding to Claim 29. Claim 53 recites:

> 53. (Previously Presented) A personal key server for controlling access to digital data of a file in a file system having a personal key server, comprising:
> means for receiving a request from a requestor to create a file header associated with the file, the request containing an **encryption key utilized to encrypt the digital data**, the encryption key being encrypted with a **personal key**;
> means for encrypting the encrypted encryption key with a **control key** to provide the file header containing an encryption key encrypted with both a personal key and a control key; and
> means for returning the file header to the requestor.

Claim 53, emphasis added.

Claim 66 is a computer program product claim corresponding to Claim 29. Claim 66 recites:

> 66. (Previously Presented) A computer program product for controlling access to digital data of a file in a file system having a personal key server, comprising:
> computer readable program code that receives a request from a requestor to create a file header associated with the file, the request containing an **encryption key utilized to encrypt the digital data**, the encryption key being encrypted with a **personal key**;
> computer readable program code that encrypts the encrypted encryption key with a **control key** to provide the file header containing an encryption key encrypted with both a personal key and a control key; and
> computer readable program code that returns the file header to the requestor.

Claim 66, emphasis added.

Thus, in embodiments of the present invention as recited in Claims 53 and 66, three keys are used in the same manner as recited in the method Claim 29. Applicants submit that a system for performing the operations of Claim 29 and computer program code that performs the operations of Claim 29 are patentable over the cited references for substantially the same reasons that Claim 29 is patentable. In particular, Claims 53 and 66 recite that the first key is an encryption key utilized to encrypt the digital data. The second key is the personal key utilized to encrypt the encryption key. The third key is the control key that is used to encrypt the encrypted encryption key.

Applicants submit that merely because a processor can be a "means" or a program may contain "program code" does not mean that just any processor or just any program teaches the inventions recited in Claims 53 and 66. For a processor to be relevant, it must be able to provide the specific functionality recited in Claim 53. For a program to be relevant, it must include code that performs the specific functions recited in Claim 66. Accordingly, Applicants submit that Claims 53 and 66, and the claims that depend from these claims, are patentable over the cited references for the reasons discussed above with reference to Claim 29.

Claims 41 and 65

In responding to Applicants' arguments that Claims 41 and 65 are patentable for reasons analogous to those of Claim 17, the Final Action states that these claims are not allowable "because the claimed invention could be exercised in a program only and the text in the claims has no affect on the processor." Final Action, p. 2. Applicants do not understand what this reason refers to but submit that Claims 41 and 65 are patentable as they are system and computer program product claims corresponding to allowed Claim 17.

For example, allowed Claim 17 recites:

17. (Original)   A method for controlling access to digital data of a file utilizing a file system including a personal key client, wherein the personal key client carries out the steps of:
generating an encryption key;
encrypting the digital data of the file with the encryption key;

obtaining a password associated with the file;
generating a personal key from the password associated with the file;
encrypting the encryption key with the personal key;
incorporating in a file header the encryption key encrypted with the personal key;
requesting encryption of the file header with a control key;
receiving the file header encrypted with the control key;
associating the file header with the file; and
storing the file header and the encrypted digital data of the file at a file server.

Rejected Claim 41 recites:

41.   (Original)   A personal key client for controlling access to digital data of a file utilizing a file system, comprising:
means for generating an encryption key;
means for encrypting the digital data of the file with the encryption key;
means for obtaining a password associated with the file;
means for generating a personal key from the password associated with the file;
means for encrypting the encryption key with the personal key;
means for incorporating in a file header the encryption key encrypted with the personal key;
means for requesting encryption of the file header with a control key;
means for receiving the file header encrypted with the control key;
means for associating the file header with the file; and
means for storing the file header and the encrypted digital data of the file at a file server.

Rejected Claim 65 recites:

65.   (Original)   A computer program product for controlling access to digital data of a file utilizing a file system including a personal key client, comprising:
a computer readable storage media having computer readable program code embodied therein, the computer readable program code comprising:
computer readable program code that generates an encryption key;
computer readable program code that encrypts the digital data of the file with the encryption key;
computer readable program code that obtains a password associated with the file;
computer readable program code that generates a personal key from the password associated with the file;
computer readable program code that encrypts the encryption key with the personal key;
computer readable program code that incorporates in a file header the encryption key encrypted with the personal key;

computer readable program code that requests encryption of the file header with a control key;

computer readable program code that receives the file header encrypted with the control key;

computer readable program code that associates the file header with the file; and

computer readable program code that stores the file header and the encrypted digital data of the file at a file server.

Thus, in embodiments of the present invention as recited in Claims 41 and 65, three keys are used in the same manner as recited in the method Claim 17. Applicants submit that means for carrying out the operations of Claim 17 and computer program code that performs the operations of Claim 17 are patentable over the cited references for substantially the same reasons that Claim 17 is patentable. In particular, both Claims 41 and 65 recite that a first key (the encryption key) is used to encrypt the digital data. A second key (the personal key), that is generated from the password, is used to encrypt the first key. The first key, encrypted with the second key, is incorporated in a file header and that file header is encrypted with a third key (the control key). By encrypting the encryption key with two different keys, file access may be controlled both by the owner of the personal key and the owner of the control key.

Applicants submit that merely because a processor can be a "means" or a program may contain "program code" does not mean that just any processor or just any program teaches the inventions recited in Claims 41 and 65. For a processor to be relevant, it must be able to provide the specific functionality recited in Claim 41. For a program to be relevant, it must include code that performs the specific functions recited in Claim 65. Accordingly, Applicants submit that Claims 41 and 65, and the claims that depend from these claims, are patentable over the cited references for the reasons discussed above.

The Dependent Claims

Applicants submit that the dependent claims are patentable at least as depending from a patentable base claim.

The Claims Are Not Obvious

Claims 45-47 stand rejected under 35 U.S.C. § 103 as obvious in light of Narasimhalu and United States Patent No. 6,105,131 to Carroll (hereinafter "Carroll"). Claims 30 and 55 stand rejected under 35 U.S.C. § 103 as obvious in light of Narasimhalu and United States Patent No. 6,678,731 to Howard et al. (hereinafter "Howard"). Applicants submit that these claims are patentable at least as depending from a patentable base claim.

Conclusion

In light of the above discussion, Applicants submit that the present application is in condition for allowance, which action is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

Timothy J. O'Sullivan
Registration No. 35,632

USPTO Customer No. 46589

Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401